Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1731 08/21/15

~ Stop Using Ad-blockers ~ ~ US Delays ICANN Plan

-* Cheating Site Includes Pols! *-
-* â Facebook Spreaderâ Hacker Pleads! *-
-* Meet The Worldâ s Most Dangerous Geeks! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, I have this weekâ s issue out at a reasonable time, but weâ re still running into â problemsâ doing
a few things with the magazine. As I mentioned last week, I had some problems with my PC. Turns out
that the problem is the motherboard is shot. So, Iâ m looking to replace the PC. Iâ ve been trying to
produce the magazine using Mac software, but I havenâ t been as successful as I â d like. Using the PC
for a number of years, Iâ ve been accustomed with various PC tools to get everything done, and done
efficiently and well! So, until I work things out using the Mac, or replace the PC (and software),
the magazine may not look exactly as it has in the past. And, I havenâ t been able to fine-tune the
web versions, so those will not be available for awhile!

Until next timeâ ƒ

=~=~=~=

Firebee Update News

Not a whole lot to report in this installment.´ Last submission I discussed my failed CF Card, what I went through to finally getting that resolved to be up and running in MiNT.´ Since then I have just been exploring the software that comes in the FireBee MiNT setup.´ I have also been testing out my favorite Atari software that I used years ago on my TT on the FireBee.´ Lastly I have been trying out newer Atari software that I have been coming across and trying that out too.

Here is some feedback on my limited use of the FireBee up to this point.

Things I like :

Speed â The FireBee feels fast to me with the software I am running on it so far.
Networking â With any computer I am using now having TCP/IP and Ethernet is a must.´ Currently the only network activity I have been doing is surfing the Web

with the included NetSurf browser and HighWire browser.´ I have not setup an e mail client yet or tried to connect to any computers on my network.

USB â Though I haven't tried a thumb drive yet being able to use many USB keyb oards and mice is nice.´ Just think of if you spill something on your keyboard or it just quits.´ You can use just about any USB keyboard and get it cheaply.´ Plus if you don't like the feel of the keyboard you can easily swap it out wit h one you like.

Video Modes -´ To me the Atari line of computers always had strange video resol utions.´ I understand that there was the 32K limitation on the ST and the TT an d Falcon had more capability but still on my TT 640x480x16 colors was not ideal for me.´ Once I acquired an Atari´ TTM195 1280x960x2 color monitor I mostly us ed that because of the higher resolution.´ With the FireBee the limitation I am facing is the monitor and not the FireBee.´ Currently I am using a 15 inch LCD that can do 1024x768.´ Yes I would like to run a higher resolution but I do no t have any larger spare monitors laying around right now.

Computer Case â I like the looks of this case.´ Someone put a lot of effort i n the design of the case.´ All the ports are clearly marked.

Support : As you have read I did run into some initial problems with the Firebee .´ Some of it was my own doing and some of it was not.´ I got great support fr om the user community.´ Initially via email directly from the ACP web site and now mostly through http://www.atari-forum.com/ forums.´ User community support has been great with the questions I have asked.

Complaints :

Video - Really the only one complaint I have with the FireBee is the screen scro lling.´ It is not as smooth as it is on other computers I am using.´ Depending on how much I have on the screen it can get jerky when scrolling.´ I am runnin g 1024x768x32bit.´ I have read a couple of threads on this.´ I don't have them book marked or can find them right now so I can't share them in this submission .´ In simple terms it has to deal with the optimization of the video routines.´ ´ Once someone gets this resolved a simple Firmware update to existing FireBee s will fix this.

Lastly as already posted in the news section of AONE on August 15, 2015 was the relaunch of the much improved FireBee.org Website.´ The site now has much more and better formatted information on the FireBee.´ More exciting is that after o ver a year of no FireBee's being available for purchase pre-orders on the 2nd Se ries FireBee is going on right now.´ If you had an interest in purchasing a Fir eBee but couldn't get one now is the time to pre-order one.´ For more informati on on on the FireBee or to pre-order please go to http://firebee.org/

The Atari Coldfire Project

The Atari Coldfire Project proudly presents:

http://firebee.org

=~=~=~=

->In This Week’s Gaming Section - Retail Video Game Industry Bidding Farewell to Xbox 360, PS3
"""""""""""""""""""""""""""""""" Chomp Forever in Addictive â Pac-Man 256â !

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Retail Video Game Industry Begins Bidding Farewell to Xbox 360, PS3

The end of an era is upon us.

Microsoft’s Xbox 360 and Sony’s PlayStation 3 video game consoles are on their way out and the game industry appears ready to move on.

That’s according to the data in the latest report from industry tracker NPD Group.

After more than a year and a half of fluctuations and uncertainty with the arrival of new hardware from Microsoft and Sony, the US retail game industry grew in July - its second consecutive month of growth, according to NPD. Overall sales of game hardware, software and accessories grew 6 percent while hardware sales rose 2 percent, despite a steep 56 percent dropoff in sales of the older Xbox 360 and PS3.

Such a dropoff has in previous months dragged hardware sales down into double-digit declines on a percentage basis. But sales of the newer Xbox One and PlayStation 4 consoles are starting to offset those declines.

The end of the Xbox 360 and PS3 has been a long time coming, with Microsoft publicly stating that support for its console will end next year, while Sony has hinted that it will follow suit. Meanwhile, many game makers have publicly dropped support for older consoles. For instance, Electronic Arts’ upcoming Star Wars Battlefront space shooter with be available only for the Xbox One, PS4 and PC. The sharp dropoffs in older hardware sales reflect the lack of consumer enthusiasm for the near-decade-old devices.

Since the introduction of new game hardware from Microsoft and Sony in November 2013, the retail game industry has been struggling to stabilize itself as it transitions away from old hardware, released almost 10 years ago, to new devices released in the past two years. Sales of these upgraded consoles have been strong, but software sales have fluctuated. On the whole, game sales have tended to fall from year-ago comparisons as the industry waited for a larger number of consumers to upgrade to new hardware, which has been dependent on game makers offering compelling reasons to upgrade.

That appears to be changing now, as both newer hardware and software sales for t

hose devices begin taking up a larger chunk of the overall market. Last month, s ales of software for the Xbox One and PS4 grew 63 percent year over year, NPD sa id.

Software sales of games on discs on the whole remained flat at $184.4 million du e to a lack of new games in the middle of the summer season. The best-selling re tail game of the month was Warner Bros.' toy-film hybrid Lego: Jurassic World, f ollowed by Warner Bros.' other big summer hit, the comic-inspired Batman: Arkham Knight in second. Microsoft's pixel-building game Minecraft came in third.

Although overall game console sales rose only 2 percent in July to $202.1 millio n from this time a year ago, sales of newer hardware like the Xbox One grew 9 pe rcent. "After 21 months, combined Xbox One and PS4 hardware unit sales are close to 50 percent higher than the combined sales of Xbox 360 and PS3 after 21 month s on the market," NPD analyst Liam Callahan wrote.

Sony was pleased with the results in July thanks mostly to a special bundled ver sion of its PlayStation 4 along with Batman: Arkham Knight. The PlayStation 4 wa s yet again the top seller last month, the company said in a statement.

Sony expects the momentum to continue into the fall as it preps yet another hard ware bundle with Activision Blizzard's space shooter Destiny, which releases a l arge update in September.

Microsoft said sales of its Xbox One console were up 44 percent year over year i n July, yet it still fell behind Sony, which has brokered deals with big-name ga me makers to get exclusive hardware bundles like Destiny and Batman. Microsoft, however, is gearing up for a hardware boost of its own with the release of the n ext installment in its acclaimed sci-fi shooter franchise Halo in October.

As has been the case in previous months, sales of games over the Internet are an even brighter spot for the industry. SuperData Research, which tracks sales and deliveries over the Internet of games and game add-ons, said the market grew 12 percent in July to $1.03 billion year over year.

"The biggest growth drivers in July were mobile and PC, which combined accounted for about 60 percent of the total digital games market," wrote SuperData CEO Jo ost van Dreunen.

Chomp Forever in Addictive â Pac-Man 256â

Youâ ve played Pac-Man. Youâ ve played Ms. Pac-Man. You might have even played the ridiculous Baby Pac-Man,´ or the incredible Pac-Man Championship Edition DX , or the atrocious Pac-Man Party, which made your terrible bar mitzvah party loo k like the awesome one from Weird Science.â ¤
But if youâ re hungry for a few more Power Pellets, then by all means, go downl oad Pac-Man 256 (free for iOS, Android, and Amazon devices) immediately. Because itâ s unlike any Pac-Man game youâ ve ever played.

For starters, the gameâ s maze never ends. Pac-Man 256 is essentially an endles s runner (or, rather, eater), which means you keep playing until you die. In thi s case, that means waka-waka-waka-ing through a gigantic, dot-filled hallway str etching out to infinity while staying one chomp ahead of an ever-encroaching wav e of glitches.

That, incidentally, is a homage to the original Pac-Manâ s infamous level 256, also known as the gameâ s â kill screen.â Upon reaching this level (a feat i

n itself), a line of garbled code mars half the screen and renders the game unpl ayable. In this case, it serves to propel you forward.

What makes this not a total snoozefest is some brilliant design choices by devel oper Hipster Whale, best known as the company behind the similarly structured me gahit Crossy Road.

Youâ ll be chased by ghosts, naturally, but they behave strangely. Occasionally theyâ ll appear in a line or emerge from a glitch cloud. Classic Pac-Man fruit s like cherries and peaches are now score multipliers. Power Pellets still turn the ghosts blue, but even handier are random power-ups like a wicked laser beam and a freeze bomb. Forget trying to gobble every last dot: Pac-Man 256 is about surviving as long as possible in order to rack up a high score and show up your friends on the leaderboard.

Perhaps what I like best is that the free gameâ s in-app purchase model doesnâ t get in the way. You get play credits every 10 minutes, but even if you run ou t, you can still play, just without using power-ups. Or you can fork over some c ash to either buy new credits or get rid of the credits system entirely. I would nâ t bother with that, though. Youâ ll get plenty of play out of this game wit hout spending a dime.

Of course, I say that now. In two months I might be a few hundred quarters deep into this clever, addictive take on Pac-Man. Heaven knows it wouldnâ t be the f irst time I spent too much money on the yellow blob.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Meet The Worldâ s Most Dangerous Geeks

Jeff Moss was desperately hunting for a back door. But this time, the DEF CON fo under wasnâ t trying to hack his way into a network â he was seeking an actua l back door, a way to avoid the masses at the Las Vegas hacker fair he launched 23 years ago.

This year, attendance would top 20,000 â and all of them seemed to be crammed into the hallways of the Paris hotel, inching their way toward massive conferenc e rooms to learn how things like Android phones and connected cars can be attack ed and pwned.

Moss tried to dart through a gift shop in the Champagne Ballroom that was sellin g DEF CON paraphernalia. The doors were blocked. He looked for a rear exit in th e Versailles Ballroom next door. No dice. Rerouting, he attempted to swing wide around an information kiosk in the center of the walkway but ran smack into a wa ll of humanity.

Moss finally had to wedge his way into the thousands heading in the opposite dir ection, as DEF CON veterans greeted him with fist bumps and cries of, â Hey DT! â (His hacker handle is Dark Tangent.) At 40, Moss doesnâ t look all that dif

ferent from the teenager who was blown away by the film WarGames and decided to create a conference for like-minded souls. As he tried to hack his way through the crowd, he was verbally debugging the process that had turned his gathering of geeks into the crowd scene from The Day of the Locust.

Jeff Moss, aka Dark Tangent, holding the Uber badge given away at DEF CON 23. (Photo: Dan Tynan/Yahoo Tech)

â This is the first break of the first day in a new hotel â thatâ s why this is so screwed up,â he muttered. â Weâ ve got to create lanes flowing in each direction and make sure each track breaks at different times.â

It was yet another sign that hacker culture â even at an enter-at-your-own-peril event like DEF CON â has gone bigtime.

DEF CON started in 1993 as a farewell party in Las Vegas for one of Mossâ s hacking friends, who was leaving the country. Moss turned it into a conference/party for roughly 100 fellow hackers he had met via electronic bulletin boards. DEF CON 1 (it got its name from WarGames) debuted with a handful of talks with titles such as â To Hack or Not to Hackâ and â Future of the Computer Underground.â

The next year, Moss decided to hold the conference in Vegas again. Attendance doubled. The year after, attendance grew again. By 1997, DEF CON had become so popular among security professionals that Moss created a second conference just for them, called Black Hat. (That name is ironic: In the hacking universe, â black hatsâ are the bad guys, the ones who launch cyberattacks for personal gain or simply to be destructive.)

In its 23rd year, DEF CON is now recognized as the ultimate meetup for hackers and hacker wannabes. This yearâ s conference featured more than 100 presentations on a huge range of topics, the public demonstration of several headline-making exploits, and elaborate warnings designed to keep naive newbies at a safe distance.

â Itâ s wise to consider the public network at DEF CON profoundly hostile,â conference organizers warned in an email, offering a long list of other precautions:

- â ¢ Do not bring a phone. If you must bring one, make it a disposable â burnerâ with no personal data on it. If you must bring a smartphone, leave it in airplane mode. Do not attempt to connect it to any networks.
- â ¢ Do not plug your computer into any randomly placed network cable or your phone into someone elseâ s charger â they could be rigged to steal your information.
- â ¢ Do not attempt to log on to the conference Wi-Fi network; you could find your name projected onto the Wall of Sheep, where hackers post unencrypted logins and passwords.
- â ¢ Bring cash. If you bring a credit card, put it inside a radio-blocking pouch; otherwise, a hacker could use a scanner to read the numbers off its RFID chip. The same goes for your hotel room key.

A security-savvy colleague of mine went even further, warning me that hackers could target me in my own hotel â a solid half-mile from the conference.
â Leave your laptop in your hotel room unplugged and turned off,â he said. â Sleep mode isnâ t good enough; it needs to be powered down.â

My DEF CON survival kit: a disposable phone, a credit card shield, my press badge/record, the show guide, and a vanilla laptop containing no personal information of any kind.

For these and other reasons, DEF CON will never be confused with more corporate security conferences. Everything at DEF CON has its own perverse twist, even dow n to the badges worn by attendees. This yearâ s model was a 7-inch vinyl record , color-coded to indicate status: red for conference official, blue for speaker, yellow for media, white for everyone else.

Dozens of attendees showed up with turntables to play the badge. (You can listen to the recordings here.) On one side was a voice-altered recitation from the Ha ckerâ s Manifesto followed by a long series of numbers and touchtones. On the f lip side, Dual Coreâ s rap tribute to hacking, â All the Things.â

â This is our world nowâ ƒ the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasnâ t run by profiteering gluttons, and you call us criminals. We exploreâ ƒ and you call us criminals. We seek after knowledgeâ ƒ and you call us criminals. We exist without skin color, without nationality, wit hout religious biasâ ƒ and you call us criminals. You build atomic bombs, you wa ge wars, you murder, cheat, and lie to us and try to make us believe itâ s for our own good, yet weâ re the criminals.â

DEF CON is best known for some occasionally dramatic presentations on security v ulnerabilities. This yearâ s talks included â Scared Poopless â LTE and Your Laptop,â â Confessions of a Professional Cyber Stalker,â and â I Will Kil l Youâ (how to hack public records to indicate someone has died).

Beyond that, DEF CON offers a series of â villages,â where attendees can lear n how to pick locks, unseal and reseal tamperproof packaging, hack into smart ap pliances, talk their way out of interrogation rooms, and more. Itâ s like a Ren aissance faire for uber-geeks.

True to its WarGames heritage, the conference is also filled with games and cont ests â like Capture the Flag, where 15 teams spend 72 hours attempting to comm andeer a network server and then defend it against other attackers, or Hacker Je opardy, where contestants answer nerdy questions while drinking copious amounts of beer and being assaulted with silly string before an audience of 2,000.

Winners of the most difficult contests at DEF CON 23 receive a custom glow-in-th e-dark Uber badge, allegedly containing trace elements of uranium 238 and trinit ite left over from the first nuclear tests at Los Alamos. They also earn a free pass to all subsequent DEF CONs for the rest of their lives.

Show DEF CON attendees a lock, and they will pick it. Give them an encrypted pas sword, and they will crack it. Present them with an allegedly secure network, an d they will prove that itâ s a lot more porous than you think. Whether theyâ r e white hats, black hats, or somewhere in between, DEF CON attendees gleefully e mbrace their own outlaw image. That has led to a complicated relationship with b oth government and big business.

In 2001, the FBI arrested Russian hacker Dmitry Sklyarov at DEF CON shortly afte r he demonstrated how to circumvent the encryption built into Adobeâ s e-book r eader. In 2005, Cisco attempted to prevent security researcher Michael Lynn from presenting a talk on vulnerabilities inside the companyâ s network routers. Th ree years later, the Massachusetts Bay Transit Authority sued three MIT students to keep them from revealing how they managed to hack Bostonâ s transit system to ride for free.

Some corporations â but not all â have realized itâ s better to have these people as friends than as potential enemies, and now reward researchers for iden tifying security bugs inside their products.

In October 2014, after security researchers Charlie Miller and Chris Valasek successfully gained control of a 2014 Jeep Cherokee via the Internet, they privately broke the news to executives from Fiat Chrysler Automobiles (FCA). Months later, after FCA had done nothing to address the problem, the pair shared their findings with Wired journalist Andy Greenberg. Within a week of the Wired story appearing, FCA issued a recall for the 1.4 million cars affected by the vulnerability. Miller and Valasek presented their findings at both DEF CON 23 and its more buttoned-down sibling, Black Hat.

At last yearâ s DEF CON, the duo revealed a list of 16 Chrysler and GM cars that could be vulnerable to attack; the Jeep was the most promising candidate. ´

â If Chrysler had attended DEF CON a few years ago, they could have saved themselves a boatload of money [from the recall],â says Winn Schwartau, a security consultant and author who says heâ s attended every DEF CON since the first in 1993.

After the Tesla Model S was hacked, the company worked with researchers to patch the holes they found.

By contrast, when Marc Rogers and Kevin Mahaffey demonstrated how to hack the internal network of a Tesla Model S, the electric carmaker proved far more welcoming. The company loaned a Model S to this yearâ s Car Hacking Village, and Chief Technical Officer JB Straubel shared a celebratory shot of whiskey on stage with the researchers â a DEF CON ritual normally reserved for first-time speakers.

The showâ s relationship with the federal government is even more complex. After years of encouraging the game â Spot the Fed,â where attendees would identify government employees quietly lurking in their midst, the show became fertile recruiting territory for three-letter federal agencies seeking to boost their cyber-IQ. In 2012, former National Security Agency Director Gen. Keith Alexander even delivered a keynote address. A year later, after Edward Snowden revealed that the agency spied on millions of American citizens, Moss politely requested that the feds refrain from attending.

Lately, Uncle Samâ s wary relationship with hackers appears ready to thaw, at least at some agencies. This year, the Federal Trade Commission presented a talk titled â How to Hack Government: Technologists as Policy Makers.â For the past two years, the agency also asked DEF CON attendees to help them develop apps to monitor and trace robocalls.

â Technologists can and should play a vital role in shaping tech policy,â says FTC Commissioner Terrell McSweeny. â A lot of people who attend DEF CON and are in the security research community connect with the FTCâ s mission to protect consumers. So we made a pitch to them to either join us (literally, apply for a job) or help us (come tell us about their research).â

During his keynote, Moss asked a packed room how many were there for the first time. Roughly a third of us raised our hands. In fact, attendance was 25 percent higher than last year, according to show organizers.

The fact is, hacking has gone mainstream â at least in pop culture. But the image of hackers that comes out of Hollywood is, Moss says, highly romanticized.

â In the early days, any time a movie or TV show had a hacking reference we all got really excited about it â â Oh my gosh, somebody knows what weâ re doing,â â he says. â Now thereâ s a token hacker in every show whoâ s just there to tap on a keyboard and move the plot along.â

In Mr. Robot, actor Rami Malek plays Elliot Alderson, a socially awkward securit y engineer turned hacker vigilante.

(The exception, says Moss: USA Networkâ s Mr. Robot, which features a vigilante hacker who makes up in social conscience what he lacks in social skills. That, Moss says, is probably the closest the entertainment industry has come to gettin g it right.)

And while the network at DEF CON may be â profoundly hostile,â the attendees are not. Itâ s still a relatively small tribe, but itâ s growing, with members hip open to anyone with intense curiosity and a high tolerance for geekiness.

â The world needs to quit being so scared of these guys,â says Schwartau. â The perception that this group is the one doing the breaches at Home Depot or So ny or Target is just wrong, wrong, wrong. The people who go to DEF CON are the c yberpriests, trying to keep things honest.â

In short, hackers deserve respect. And if theyâ re not careful, one day they ma y even get it.

Hacker Pleads Guilty to ’Facebook Spreader’ Scam

A New Yorker who infiltrated thousands of computers in order to run a lucrative spam bot pleaded guilty in U.S. District Court.

Eric Crocker, of Binghamton, N.Y., was one of a dozen people charged over the su mmer for his participation in a computer hacking forum known as Darkode.

Operating under the pseudonym "Phastman," the 29-year-old pleaded guilty on Mond ay to one count of violating the CAN-SPAM Act. He used a hacking tool called Fac ebook Spreader, which infected Facebook-connected PCs and turned them into bots. Crocker then sold access to his bot, which scammers used to send out massive am ounts of spam.

According to a Reddit post submitted a year ago, the virus sends a Facebook mess age to the affected users’ friends, with an attached malware file that runs as s oon as it’s clicked. Cybercriminals then bought, sold, traded, and shared inform ation and tools on the password-protected Darkode forum.

Crocker and other hackers made about $200 to $300 for every 10,000 computer infe ctions, according to Reuters, a scheme that likely earned Crocker upwards of $21 million.

He now faces up to three years in prison or a fine of $250,000, possibly both, t he FBI said. Sentencing is scheduled for Nov. 23.

"This operation is a great example of what international law enforcement can acc omplish when we work closely together to neutralize a global cybercrime marketpl ace," Assistant Attorney General Leslie Caldwell said in July.

Cheating Website Subscribers Included WH, Congress Workers

Hundreds of U.S. government employees â including some with sensitive jobs in the White House, Congress and law enforcement agencies â used Internet connections in their federal offices to access and pay membership fees to the cheating website Ashley Madison, The Associated Press has learned.

The AP traced many of the accounts exposed by hackers back to federal workers. They included at least two assistant U.S. attorneys; an information technology administrator in the Executive Office of the President; a division chief, an investigator and a trial attorney in the Justice Department; a government hacker at the Homeland Security Department and another DHS employee who indicated he worked on a U.S. counterterrorism response team.

Few actually paid for their services with their government email accounts. But AP traced their government Internet connections â logged by the website over five years â and reviewed their credit-card transactions to identify them. They included workers at more than two dozen Obama administration agencies, including the departments of State, Defense, Justice, Energy, Treasury, Transportation and Homeland Security. Others came from House or Senate computer networks.

The AP is not naming the government subscribers it found because they are not elected officials or accused of a crime.

Hackers this week released detailed records on millions of people registered with the website one month after the break-in at Ashley Madison’s parent company, Toronto-based Avid Life Media Inc. The website â whose slogan is, "Life is short. Have an affair" â is marketed to facilitate extramarital affairs.

Many federal customers appeared to use non-government email addresses with handles such as "sexlessmarriage," ’’soontobesingle" or "latinlovers." Some Justice Department employees appeared to use pre-paid credit cards to help preserve their anonymity but connected to the service from their office computers.

"I was doing some things I shouldn’t have been doing," a Justice Department investigator told the AP. Asked about the threat of blackmail, the investigator said if prompted he would reveal his actions to his family and employer to prevent it. "I’ve worked too hard all my life to be a victim of blackmail. That wouldn’t happen," he said. He spoke on condition of anonymity because he was deeply embarrassed and not authorized by the government to speak to reporters using his name.

The AP’s analysis also found hundreds of transactions associated with Department of Defense networks, either at the Pentagon or from armed services connections elsewhere.
Defense Secretary Ash Carter confirmed the Pentagon was looking into the list of people who used military email addresses. Adultery can be a criminal offense under the Uniform Code of Military Justice.

"I’m aware it," Carter said. "Of course it’s an issue because conduct is very important. And we expect good conduct on the part of our people. ... The services are looking into it and as well they should be. Absolutely."

The AP’s review was the first to reveal that federal workers used their office systems to access the site, based on their Internet Protocol addresses associated with credit card transactions. It focused on searching for government employees in especially sensitive positions who could perhaps become blackmail targets. The government hacker at the Homeland Security Department, who did not respond to phone or email messages, included photographs of his wife and infant son on his Facebook page.

One assistant U.S. attorney declined through a spokesman to speak to the AP, and

another did not return phone or email messages.

A White House spokesman said Thursday he could not immediately comment on the matter. The IT administrator in the White House did not return email messages.

Federal policies vary for employees by agency as to whether they would be permitted during work hours to use websites like Ashley Madison, which could fall under the same category as dating websites. But it raises questions about what personal business is acceptable â and what websites are OK to visit â for government workers on taxpayer time, especially employees who could face blackmail.

The Homeland Security Department rules for use of work computers say the devices should be used for only for official purposes, though "limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of network services." Employees are barred from using government computers to access "inappropriate sites" including those that are "obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable."

The hackers who took credit for the break-in had accused the website’s owners of deceit and incompetence, and said the company refused to bow to their demands to close the site. Avid Life released a statement calling the hackers criminals. It added that law enforcement in both the U.S. and Canada is investigating and declined comment beyond its statement Tuesday that it was investigating the hackers’ claims.

China Vows To â Clean The Internet" in Cybercrime Crackdown, 15,000 Arrested

The Ministry of Public Security in China said this week that 15,000 people have been arrested since the launch of a major anti-cybercrime operation called "cleaning the internet."

So far, the six-month´ operation, launched in July, has produced investigations of over 7400 cases of cybercrime and 66,000 websites.

In an announcement on its website, the ministry said the arrests were for crimes that "jeopardized internet security," and described in detail a handful of cases, ranging from network attacks and website intrusions to sophisticated frauds.

Two of the investigations cited involved hacking websites to display advertising for gambling sites: the compromised websites included a pharmaceutical company and more than 40 "important news sites."

The ministry also described one case where hackers used phony ads on Baidu, China’s largest search engine, to scam people who thought they were calling an airline customer service line.

Another case involved hackers sending mass SMS messages containing malicious links to take control of mobile devices.

That case sounds a lot like one we reported on Naked Security in August 2014, where a Chinese teenager was arrested for spreading a mobile SMS virus that infected 100,000 mobile devices.

The ministry said another investigation resulted in the arrests of six members of a gang responsible for sending massive amounts of SMS spam from Wi-Fi base sta

tions.

In a similar case last year, Chinese authorities arrested over 1500 SMS spammers who used mobile base stations to blast mobile phones in range with text messages.

According to a report from Reuters, the current crackdown also targets websites providing "illegal and harmful information" as well as ads for pornography, firearms and explosives.
Although the ministry said the campaign is focused on crushing organized cybergangs in the country, some analysts suspect China’s broad cybercrime law could sweep up activists and dissidents along with the crooks.

While China’s strict internet censorship rules prohibit Chinese citizens from accessing many foreign websites - a policy enforced by the "Great Firewall" - speech is also censored in the Chinese media and on Chinese social networks.

China’s internet censorship laws allow the police to shut down websites that spread "false rumors" or "incite panic."

According to Al Jazeera, the Cyberspace Administration of China shut down or suspended dozens of news websites for spreading false information about the recent chemical explosions in the port city of Tinjian that left more than 100 people dead.

In what seems like an attempt at transparency, Chinese police launched an "internet inspection" branch in June of this year, consisting of police in 50 cities using public accounts on social networks such as WeChat and Weibo.

These officers will "deter and prevent cybercrimes and improper words and deeds online," while also accepting crime tips and warning those involved in "minor offenses," according to the government-run news agency Xinhua.

In 2015 alone, Chinese authorities have deleted 758,000 pieces of "illegal and criminous information" from Chinese websites, and have investigated over 70,000 cases of cybercrime, Xinhua reported.

Amazon Bans Flash Ads - But Not for the Reason You May Have Hoped!

Websites with cool interactive content like games used to go for Java.

By embedding a special sort of Java program called an applet in your website, you could add a bit more pizazz than your competitors could manage with plain old HTML.

Then came Adobe Flash, using a programming language called ActionScript instead of Java, but with the same ultimate idea: multi-platform, cross-browser, web-based, real-time, on-line multimedia coolness.

There were downsides to Java and Flash from the start, of course, namely that:

- â ¢ They were "someone else’s" standards, rather than web ones.
- â ¢ They required you to install and manage additional plugins in your browser.
- â ¢ They inevitably opened up additional security holes.
- â ¢ Cybercrooks fell in love with Java and Flash security holes because they often worked in every browser, leading to true "cross-platform" attacks.

Eventually, browser makers and web standards-setters agreed on an alternative ap
proach, called HTML5, that would (or at least could) make both Java and Flash re
dundant by giving web programmers a way to do cool multimedia stuff right inside
 the browser.

As a result, these days you can just use JavaScript in your interactive web page
s, instead of using Java or ActionScript.

â Java and JavaScript are completely different. As a recent Naked Security com
mentator pointed out, "Java" and "JavaScript" are no more strongly related than
"Car" and "Carpet." They simply start with the same letters.

Sure, HTML5 increases the so-called "attack surface area" of your browser becaus
e there are now more tricks you can pull off with JavaScript, and there is more
code in the background to go wrong.

But every modern browser supports JavaScript and HTML5 anyway; HTML5 can do the
job of Java and Flash; and many if not most websites support HTML5, even if they
 also support Java or Flash.

Simply put, almost all of us can live without Java or Flash in our browsers, alm
ost all of the time.

Indeed, most of us do live without Java in our browsers these days, because Orac
le, which owns Java, no longer enables the Java applet web browser plugin by def
ault when you install the Java product.

Java is mainly used for applications, full-blown software programs that you inst
all locally, so support for in-browser applets is rarely necessary these days.

But Flash has proved harder to eject from the world’s browsers, with lots of peo
ple keeping it installed and turned on, and often insisting that they need it, e
ven when they don’t.

Apple was the first big brand name to take against Flash in a big way, by the si
mple expedient of banning it altogether on iPads and iPhones.

If you have an iDevice, you don’t have Flash, and that’s that: it’s all done wit
h HTML5 instead.

Facebook jumped into the anti-Flash wars recently, too, with its newly-appointed
 CSO coming out swinging on Twitter.

Alex Stamos publicly demanded that Adobe should act to kill off Flash, and to se
t a date by which all browsers would refuse to support it.

Of course, that was just a Twitter rant.

Facebook doesn’t yet seem to share its CSO’s strident views, because the company
 didn’t back him up, and still makes use of Flash in your browser if you have it
 installed.

That’s annoying for those who want to convince the world that Flash is largely s
uperfluous, and thus an unnecessary security risk.

Sites that use Flash "because they can", instead of just moving to HTML5 for eve
rything, tend to reinforce users who still think they need Flash, even when turn
ing it off would make no visible difference.

So Flash naysayers will welcome Amazon’s recent announcement:

Beginning September 1, 2015, Amazon no longer accepts Flash ads on Amazon.com, AAP, and various IAB standard placements across owned and operated domains.

This is driven by recent browser setting updates from Google Chrome, and existing browser settings from Mozilla Firefox and Apple Safari, that limits Flash content displayed on web pages. This change ensures customers continue to have a positive, consistent experience across Amazon and its affiliates, and that ads displayed across the site function properly for optimal performance.

Interestingly that Amazon hasn’t gone all out by banning Flash because of its security risk - the "added attack surface area" it brings to your browser.

Amazon is blaming, if that’s the right word, three of the world’s Big Four browsers instead, because they no longer play Flash ads automatically by default.

Indeed, Amazon’s explicit reason for ditching Flash seems to be that it will improve the consistency of your ad-viewing experience, meaning that your browser’s "click-to-play" Flash option will no longer act as a sort-of implicit ad blocker.

Ironically, even though Amazon’s announcement means that some users will start seeing ads that didn’t appear before, it may actually help to distance Amazon from Adobe’s recent (and rather unpopular) suggestion that ad blockers are a Bad Thing and could cost our economy $22,000,000,000 this year.

Nevertheless, Amazon has banned Flash ads, and that’s that!

FCC Fines Company $750,000 for Disabling Conference Hotspots

The US Federal Communications Commission (FCC) has fined a telecommunications company a whopping $750,000 (nearly ´£500,000) for blocking consumers’ Wi-Fi "personal hotspots" at convention centers around the country.

The FCC announced the fine on Tuesday, saying that Smart City Networks had been blocking personal hotspots being used by convention visitors and exhibitors who used their own data plans rather than paying Smart City "substantial fees" to use its Wi-Fi service.

Most modern mobile phones have a connection-sharing option (personal hotspot on iOS, portable hotspot on Android and internet sharing on Windows Phone) that lets you hook up one or more devices to the phone via Wi-Fi, and then connect onwards to the internet via the phone’s 3G or LTE data connection.

The FCC’s release quotes Travis LeBlanc, Chief of its Enforcement Bureau:

It is unacceptable for any company to charge consumers exorbitant fees to access the Internet while at the same time blocking them from using their own personal Wi-Fi hotspots to access the Internet.

All companies who seek to use technologies that block FCC-approved Wi-Fi connections are on notice that such practices are patently unlawful.

The company’s response: "We didn’t know that!"

Smart City said in a release that it hadn’t known that it was against FCC rules

to use standard, out-of-the-box technology in order to prevent wireless devices from disrupting the operations of neighboring exhibitors on convention floors, having received no prior notice before the FCC contacted it in October 2014.

That’s also when the FCC slapped Marriott with a $600,000 fine (nearly ´£400,000) for blocking Wi-Fi access at its Gaylord Opryland Resort and Convention Center in Nashville, Tennessee.

Marriott didn’t go down without a fight: it banded together with the American Hotel and Lodging Association to try to talk the FCC into changing the rules and allowing it to keep blocking personal hotspots.

Marriott gave in and stopped blocking hotspots in January 2015, although it said at the time that it was going to keep on trying to get the FCC’s blessings on blocking.

The hotel chain maintained that it hadn’t intended to block personal hotspots in guests’ rooms or in lobbies, but that it was asking the FCC to allow the practice in conference rooms or other meeting spaces.

"It’s all about Wi-Fi security," Marriott said: specifically, ensuring that guests using its Wi-Fi were protected from rogue wireless hotspots that it said could degrade service, from "insidious cyber-attacks", and from identity theft.

"Riiiiight," skeptics said, "it’s about security, not about what the FCC said was a charge of $250 to $1,000 per device to get onto the internet at a Marriott property."

For its part, Smart City said that blocking hotspots resulted in "significantly less" than 1% of all devices being deauthenticated´ and that these same technologies are "widely used by major convention centers across the globe as well as many federal agencies."

While Smart City thinks it has legal standing to fight the fine, its president, Mark Haley, said in the company’s release that the battle would be too costly and too much of a distraction.

But even if Smart City thinks it might have had a chance to fight, given that its case goes back to 2014, there’s no way to say "I didn’t know that" any more.

Back in January 2015, the FCC published DA 15-113A1, its first Enforcement Advisory of the year.

Let’s just say that this notice didn’t exactly mince its words:

Sites Try Polite Approach in Asking Readers To Stop Using Ad-blockers

Ad-blocking has become one of the main scourges of the online publishing and advertising industries.

Software tools that can detect web advertisements and then block them from users â view have become increasingly popular as consumers fret about things like data collection or the glut of advertising slowing down Web pages.

But ad-blockers have become a major problem for publishers because most of the free content distributed online is supported by advertising revenue. One recent report suggested the issue would lead to $22bn in lost revenue this year as one o

ut of three internet users now employed some software to block ads.

As ad-blocking spreads across the internet, publishers have tried different stra tegies to deal with the problem, everything from completely disallowing ad-block ing users from viewing content on their sites to paying anti-ad-blocking firms t o block the blockers.

Some publishers, however, have taken a softer approach: appealing directly to re aders.

For instance, Wired in recent months has tested various versions of diplomacy, a sking readers to "please do us a solid and disable your ad-blocker". The message appears on the Web page where an ad normally would.

"We figured the best place to start with that is just to ask," said Mark McClusk y, head of operations at Wired, which is owned by Condˆ' Nast. Mr McClusky said it was important to be straightforward with Wiredâ s "very tech-savvy audience" .

"Itâ s too early to tell if the appeals are working, and Wired is still testing how best to communicate with its readers about ad-blocking," Mr McClusky said.

The Guardian also makes its case to readers directly with a message that reads: "We notice youâ ve got an ad-blocker switched on. Perhaps youâ d like to suppo rt the Guardian in another way?" It directs visitors to a link to become a "supp orter", or donor, to the Guardian.

"Thereâ s no silver bullet to mitigate against ad-blocking, which is why weâ r e running tests to encourage users of ad-blockers to fund high-quality journalis m in other ways," Guardian US CEO Eamonn Store said in an e-mailed statement.

Others sound a more dire tone, like free gaming network GameBanana.com. "Without ads, we will not survive," its appeal says.

Tom Pittlik, founder of the site, said that 30% of page views in April were load ed by browsers with ad-blocking enabled.

Mr Pittlik said he was limited creatively when it came to the appeals, since the y were background images over which an ad should appear. That presented a challe nge when it came to making the message more dynamic than just text.

"Young audiences definitely forget how media sites work and support themselves," Mr Pittlik said. "Though advertisers are equally to blame for a history of irre levancy, intrusiveness, browser-crashing ads and malware."

Given that the use of ad-blockers comes down more to fairness than legality, the question is whether begging for mercy actually works.

Sean Blanchfield, CEO of ad-blocking measurement service PageFair, said it did n ot.
In a blog post last year, PageFair said it ran 576 different appeals on 220 webs ites, but found that only 0.33% of ad-blockers that saw an appeal added sites to their approved site list. And a third of those people eventually removed the ex emption.

Mr Blanchfield said the results were "not encouraging" and, on the whole, appeal s could not "counter the organic growth rate of ad-blocking."

Getting ad-blockers to change their default behaviour was difficult, Mr Blanchfi eld said.

U.S. Delays Plans To Cede Oversight of Internet Administrator to 2016

The U.S. Department of Commerce on Monday said it would delay plans to give up oversight of a non-profit agency that manages the Internet's infrastructure until September 2016.

The government body said it plans to renew its contract with the Internet Corporation for Assigned Names and Numbers (ICANN) for one year.

Since 1998, the United States has contracted out, through the Commerce Department, the management of the master database for top-level domain names like .com and .net and their corresponding numeric addresses to ICANN.

The Commerce Department has long expected to phase out its oversight and initially planned to do it at the end of the current ICANN contract in September.

Assistant Secretary for Communications and Information Lawrence Strickling wrote in a blog post that the Commerce Department reached its decision after the groups developing the transition documents said they would need at least until September 2016 to complete required processes and implement their proposals. (http://1.usa.gov/1NBL9D1)

He said the department on Friday notified Congress that it plans to extend the contract with ICANN until Sept. 30, 2016.

"It has become increasingly apparent over the last few months that the community needs time to complete its work, have the plan reviewed by the U.S. government and then implement it if it is approved," Strickling wrote.

Strickling also said there were options to extend the contract by up to three more years, if needed.

Some Republican lawmakers have raised concerns about the plan to hand over the stewardship of the ICANN to a global multi-stakeholder body, as they fear it may allow foreign governments that do not adhere to principles of free speech to influence the body.

Facebook Tops Social Pack in US, Twitter Lags

Facebook remains the dominant social network for US Internet users, while Twitter has failed to keep apace with rivals like Instagram and Pinterest, a study showed Wednesday.

The Pew Research Center report found 72 percent of Americans who are online currently use Facebook, a modest uptick of one percentage point from a year ago and five points higher than in 2012.

Because the vast majority of Americans use the Internet, the figures suggest 62 percent of all US adults are on Facebook, according to Pew.

The study showed Pinterest, the bulletin-board style network, was used by 31 percent of those surveyed while Facebook-owned photo-sharing network Instagram grab

bed 28 percent, with both showing significant growth.

Twitter’s share remained stuck at 23 percent, the same level as last year, altho ugh it rose from 16 percent in 2012.

Facebook has an added advantage over its rivals because its users are "highly en gaged," according to the survey, which found 70 percent of Facebook users saying they log on daily, including 43 percent who do so several times a day.

That compared with daily engagement of 59 percent for Instagram users, 38 percen t of those on Twitter and 27 percent of Pinterest users.

LinkedIn, a social network oriented toward career enhancement, saw its user base decline to 25 percent of online adults, from 28 percent in 2014. But those who use the platform daily rose to 22 percent from 13 percent a year earlier.

Some 10 percent of online adults said they used Tumblr, the blogging platform ac quired two years ago by Yahoo. That compared with six percent the last time Pew asked in December 2012.

Tumblr is popular among younger adults with 20 percent of those between the ages of 18 and 29 reporting they use it, Pew found.

The survey mirrored the global picture for the major social networks. Facebook l ast month said its monthly active user based grew to 1.49 billion. Twitter’s use r base increased only marginally to 316 million.

Twitter’s share of US Internet users remained stuck at 23 percent, the same leve l as last year, although it rose from 16 percent in 2012.

Pew found that Facebook was notably popular among women, garnering 77 percent of those who are online, and the 18-29 age group, where 82 percent use the social network.

The Pew survey also showed considerable interest in messaging applications which allow smartphone users to bypass carrier networks.

Some 36 percent of smartphone owners said they used messaging apps such as Whats App, Kik or iMessage.

These apps are especially popular among young adults, and were used by 49 percen t of smartphone owners between the ages of 18 and 29, Pew found.

"The emergence of messaging apps is noteworthy as these communication tools serv e different social needs than traditional online social networks," said lead aut hor Maeve Duggan, a researcher at Pew.

"The data also show how swiftly an already complex terrain of interaction is bec oming more varied."

The survey found 17 percent of adult smartphone owners used apps which automatic ally delete messages to protect privacy such as Snapchat or Wickr. Among young a dults, the percentage was even higher at 41 percent.

The Pew report is based on telephone interviews conducted from March 17 to April 12 among a national sample of 1,907 adults, including 1,612 Internet users, wit h a margin of error between 2.6 and 4.6 percentage points, depending on the subg roup.

=~=~=~=